



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/698,910

10/31/2003

Robert A. Clucas

C4-1212

2965

26799

7590

04/12/2005

IP LEGAL DEPARTMENT
TYCO FIRE & SECURITY SERVICES
ONE TOWN CENTER ROAD
BOCA RATON, FL 33486

EXAMINER

HUNNINGS, TRAVIS R

ART UNIT

PAPER NUMBER

2632

DATE MAILED: 04/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

(3)

Office Action Summary	Application No. 10/698,910	Applicant(s) CLUCAS, ROBERT A.	
	Examiner Travis R Hunnings	Art Unit 2632	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 October 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Drawings

1. The drawings are objected to because of the following informalities:

Element 218 in figure 2 is incorrectly labeled "control logic" and should be changed to "control module";

Element 126 in figure 1 is not described in the specification;

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. The abstract of the disclosure is objected to because it does not clearly describe the scope of the invention in enough detail. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 22 recites the limitations "said unique identifier", "said first signal", "said second signal", "said third signal", "said fourth signal" and "said filtered signal" throughout the body of the claim. There is insufficient antecedent basis for these limitations in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1, 2, 4, 14-16, 18, 20, 23, 26 and 27 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Mawhinney (US Patent 4,646,090).

Regarding claim 1, Mawhinney discloses *Codeable Identifying Tag And Method Of Identification Thereof* that has the following claimed subject matters:

The claimed method to detect security tags comprising establishing an interrogation zone using at least two signals operating at different frequencies is met by the interrogating station transmitting two discrete frequencies toward the tag (col1 49-68);

The claimed method comprising monitoring said interrogation zone to detect a plurality of security tags, with each security tag responsive to at least one of said signals is met by the tag radiating one or both of the mixed signals to the interrogating station and the interrogating station comparing the return signal with the transmitted signals to detect the presence of the various tags (col1 49-68 col3 50-67);

The claimed method comprising determining whether to generate an alarm if a security tag is detected is met by the terminal producing a signal when a tag is detected and the terminal signal being used to trigger an alarm (col3 50-67);

The claimed method comprising generating said alarm in accordance with said determination is met by the alarm being triggered (col3 50-67).

Regarding claim 2, Mawhinney discloses all of the claimed limitations. The claimed method comprises transmitting a signal at a first frequency and transmitting a second signal at a second frequency is met by the interrogating station transmitting two signals at two discrete frequencies (col1 49-68).

Regarding claim 4, Mawhinney discloses all of the claimed limitations. The claimed method comprising receiving a third signal at a third frequency from a first security tag in response to said first and second signals, wherein said third signal is a combination of said first and second signals is met by the tag radiating a response signal at a frequency that is either the sum or difference of the transmitted signals (col1 49-68).

Regarding claim 14, Mawhinney discloses all of the claimed limitations:

The claimed security system comprising at least one antenna is met by the transmitting and receiving antennas of the interrogating station (figure 1 and col2 11-27);

The claimed system comprising a transceiver to connect to said antenna and establish an interrogation zone is inherent in the system of Mawhinney transmitting and receiving the signals from the interrogating station (col1 49-68);

The claimed system comprising a first security tag to communicate with said transceiver is met by the basic type tag responding to the frequencies transmitted by the interrogating station (col2 57-65);

The claimed system comprising a second security tag to communicate with said transceiver is met by the similar tags and various tags that are used in the system (col3 4-67);

The claimed system comprising a reader system to connect to said transceiver and to determine whether either security tag is within said interrogation zone is met by the detector/comparator circuitry comparing the received and transmitted signals to determine if a triggering signal should be produced (col1 49-68 and col3 50-67).

Regarding claim 15, Mawhinney discloses all of the claimed limitations. The claimed system wherein said reader system is configured to send an alarm signal if either security tag is within said interrogation zone is met by the detector/comparator circuit producing a trigger signal that may be used to trigger an alarm (col3 50-67).

Regarding claim 16, Mawhinney discloses all of the claimed limitations. The claimed system wherein said security system further comprises an alarm system to connect to said reader system, said alarm system to receive said alarm signal and provide an alarm in response to said alarm signal is met by the triggering signal being connected to an alarm to cause an alarm to occur (col3 50-67).

Regarding claim 18, Mawhinney discloses all of the claimed limitations. The claimed system wherein said first security tag is a radio frequency tag is met by the tag being receptive of RF signals (col1 49-68).

Regarding claim 20, Mawhinney discloses all of the claimed limitations:

The claimed security system comprising at least one antenna is met by the transmitting and receiving antennas of the interrogating station (figure 1 and col2 11-27);

The claimed system comprising a transceiver to connect to said antenna and establish an interrogation zone is inherent in the system of Mawhinney transmitting and receiving the signals from the interrogating station (col1 49-68);

The claimed system comprising a reader system to connect to said transceiver and configured to detect different security tags within said interrogation zone is met by the detector/comparator circuitry comparing the received and transmitted signals to determine if a triggering signal should be produced (col1 49-68 and col3 50-67).

Regarding claim 23, Mawhinney discloses all of the claimed limitations. The claimed system further comprising an alarm system to receive said event signal and to activate an alarm in response to said event signal is met by detector/comparator circuit producing a trigger signal that may be used to trigger an alarm (col3 50-67).

Regarding claim 26, the claim is interpreted and rejected as claim 1 stated above. The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

Regarding claim 27, the claim is interpreted and rejected as claim 2 stated above. The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

7. Claim 20 is rejected under 35 U.S.C. 102(b) as being clearly anticipated by Carney et al. (Carney; US Patent 5,446,447).

Regarding claim 20, Carney discloses the following claimed limitations:

The claimed security system comprising at least one antenna is met by the reader including an antenna (col8 65);

The claimed security system comprising a transceiver to connect to said antenna and establish an interrogation zone is inherent in the device of Carney transmitting and detecting the signals resonated by the RF tags at the reader (col8 65-67, col9 3-6 and 34-41);

The claimed security system comprising a reader system to connect to said transceiver and configured to detect different security tags is met by the tuneable band pass filters being able to detect multiple different resonant frequencies of the resonant tags (col8 65-67 and col9 34-41).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 3 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mawhinney.

Regarding claim 3, Mawhinney discloses all of the claimed limitations. It would have been obvious to use the claimed frequencies as transmitting frequencies because they are in the radio frequency signal band and the signals transmitted by the interrogating station are RF signals (col1 49-68).

Regarding claim 28, the claim is interpreted and rejected as claim 4 stated above. The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

10. Claims 1-6, 22 and 26-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carney.

Regarding claim 1, Carney discloses *RF Tagging System Including RF Tags*

With Variable Frequency Resonant Circuits that has the following claimed subject matters:

The claimed method comprising establishing an interrogating zone using at least two signals operating at different frequencies is met by the system continuously sweeping through all of the frequencies which the resonant circuits of the RF tags may be resonant (col9 3-6);

The claimed method comprising monitoring said interrogation zone to detect a plurality of security tags with each security tag responsive to at least one of said signals is met by the detector detecting the selected resonant frequencies of the RF tags that are responsive to any one of a plurality of resonant frequencies (abstract);

The claimed method comprising determining whether to generate an alarm if a security tag is detected and generating said alarm in accordance with said determination would have been obvious to one of ordinary skill in the art when an RF tag was detected because the use of RF tagging in security systems that implement anti-theft alarms are well known in the art (col1 23-31).

Regarding claim 2, Carney discloses all of the claimed limitations. The claimed method comprising transmitting a first signal at a first frequency and transmitting a second frequency at a second signal at a second frequency is met by the system

continuously sweeping through all of the frequencies which the resonant circuits of the RF tags may be resonant (col9 3-6).

Regarding claim 3, Carney discloses all of the claimed limitations. It would have been obvious to use the claimed frequencies as transmitting frequencies because they are possible frequencies that are known for RF tags to be resonant.

Regarding claim 4, Carney discloses all of the claimed limitations. The claimed method comprises receiving a third signal at a third frequency from a first security tag in response to said first and second signals, wherein said third signal is a combination of said first and second signals is met by the RF tag resonating at selected ones of the different frequencies in a predetermined time sequence corresponding to a predetermined identification code in response to the interrogation signal (abstract).

Regarding claim 5, Carney discloses all of the claimed limitations. The claimed method comprising filtering out said first signal from said third signal, determining whether said second signal remains after said filtering and sending an alarm signal if said second signal remains after said filtering is met by the reader having decoding means that includes tuneable band pass filters tuning the reader to detect each of the particular resonant frequencies of the tags (col9 34-41). The claimed sending an alarm signal if said second signal remains after said filtering would have been obvious to one of ordinary skill in the art when an RF tag was detected because the use of RF tagging

in security systems that implement anti-theft alarms are well known in the art (col1 23-31).

Regarding claim 6, Carney discloses all of the claimed limitations. The claimed method comprising receiving said alarm signal and triggering said alarm in response to said alarm signal would have been obvious to one of ordinary skill in the art when an RF tag was detected because the use of RF tagging in security systems that implement anti-theft alarms are well known in the art (col1 23-31).

Regarding claim 22, Carney discloses all of the claimed limitations. The claimed security system comprising a filter to filter out said first signal from said third signal is met by the tuneable band pass filters (col8 65-67). The claimed security system comprising a detector to determine if said second signal is present in said filtered signal is met by the tuneable band pass filters and the decoding means that determine which frequency of the RF tag is resonating at a particular time (col10 4-14). The claimed security system comprising a decoder module to decode said unique identifier from said fourth signal is met by the decoding means detecting the particular RF frequency that the tag is resonating at (col10 4-14). It would have been obvious to include an event module to generate an event signal (such as an alarm signal) in response to a signal from said detector or said decoder module when an RF tag is detected in order to operate an alarm system that is well known in the art of RF tags (col1 23-31).

Regarding claim 26, the claim is interpreted and rejected as claim 1 stated above (with regards Carney). The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

Regarding claim 27, the claim is interpreted and rejected as claim 2 stated above (with regards Carney). The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

Regarding claim 28, the claim is interpreted and rejected as claim 4 stated above (with regards Carney). The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

Regarding claim 29, the claim is interpreted and rejected as claim 5 stated above (with regards Carney). The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

Regarding claim 30, the claim is interpreted and rejected as claim 6 stated above (with regards Carney). The examiner takes official notice that it is well known in the art

to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

11. Claims 24 and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over Carney in view of Vega (US Patent 6,362,738).

Regarding claim 24, Carney discloses all of the claimed limitations except for the claimed security system comprising an inventory control system to receive said event signal and store information associated with said unique identifier. Vega discloses *Reader For Use In A Radio Frequency Identification System And Method Thereof* that teaches an RF tag reader system that is connected to a host computer that has a database that can store event information regarding the RF tags (col4 63-65 and col3 55-59). Including a host computer with a updateable database to track inventory changes for the RF tags would increase the flexibility of the system and allow a better tracking of tagged items that are used in security systems. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Carney according to the teachings of Vega to include a control system to receive said event signal and store information associated with said unique identifier.

Regarding claim 25, Carney discloses all of the claimed limitations except for the claimed security system further comprising a deactivation module to deactivate either

Art Unit: 2632

said first or second security tags. Vega teaches a deactivating module for deactivating the security tags after purchase so the security system is not set off (col4 46-48).

Adding a deactivation module to the device of Carney would help to prevent false alarms if an RF tag was inadvertently left on a validly purchased item. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Carney according to the teachings of Vega to include a deactivation module to deactivate either said first or second security tags.

12. Claims 7, 10, 12, 13, 17, 19, 21 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mawhinney in view of Vega.

Regarding claim 7, Mawhinney discloses all of the claimed limitations except for the claimed method comprises receiving a fourth signal from a second security tag in response to said second signal, said fourth signal representing security tag information stored by said second security tag. Vega teaches a combined EAS and RFID tag reader that can detect the presence of both regular EAS (RF) and RFID tags (col4 51-55). The system of Vega interrogates the RFID tag and receives a response signal that contains information that is stored in the RFID tag (col4 51-55). Modifying the system of Mawhinney to be able to detect both regular RF and also RFID security tags, and receive a signal from the RFID tag that includes information stored in the RFID tag, would increase the benefits of the system by being able to detect multiple types of tags. Therefore it would have been obvious to one of ordinary skill in the art at the time of the

invention to modify the device disclosed by Mawhinney according to the teachings of Vega to receive a fourth signal from a second security tag in response to said second signal, said fourth signal representing security tag information stored by said second security tag.

Regarding claim 10, Mawhinney discloses the following claimed limitations:

The claimed method comprising receiving a first and second signal having a first and second frequency, respectively, at a first security tag is met by the interrogating station transmitting two signals at separate frequencies to be received by a tag (col1 49-68);

The claimed method comprising transmitting a third signal from said first security tag in response to said first and second signals is met by the tag radiating a response signal at a frequency that is either the sum or difference of the transmitted signals (col1 49-68).

However, Mawhinney does not specifically disclose the claimed method comprising receiving said second signal at a second security tag and transmitting a fourth signal from said second security tag in response to said second signal, with said fourth signal representing an identifier for said second security tag and a first code. Vega teaches a combined EAS and RFID tag reader that can detect the presence of both regular EAS (RF) and RFID tags (col4 51-55). The system of Vega interrogates the RFID tag and receives a response signal that contains information that is stored in the RFID tag (first code) (col4 51-55) including the tag's identification (col3 42-44).

Modifying the system of Mawhinney to be able to detect both regular RF and also RFID security tags, and receive a signal from the RFID tag that includes information (first code) stored in the RFID tag, including the RFID identification would increase the benefits of the system by being able to detect multiple types of tags. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Mawhinney according to the teachings of Vega to receive said second signal at a second security tag and transmit a fourth signal from said second security tag in response to said second signal, with said fourth signal representing an identifier for said second security tag and a first code.

Regarding claim 12, the claim is interpreted and rejected as claim 3 stated above.

Regarding claim 13, the claim is interpreted and rejected as claim 4 stated above.

Regarding claim 17, Mawhinney discloses all of the claimed limitations except for the claimed security system wherein said second security tag is a radio frequency identification (RFID) tag, said RFID tag further comprising an identification module to provide an identifier for said second security tag and a transmitter to send a signal with said identifier to said transceiver. Vega teaches a combined EAS and RFID tag reader that can detect the presence of both regular EAS (RF) and RFID tags (col4 51-55). The

system of Vega interrogates the RFID tag and receives a response signal that contains information that is stored in the RFID tag (col4 51-55) including the tag's identification (col3 42-44). Modifying the system of Mawhinney to be able to detect RFID tags in addition to RF tags would be beneficial because the system would then be able to detect multiple different types of tags. It is obvious that an RFID tag includes an identification module to provide an identifier for said security tag and a transmitter to send a signal with said identifier to said transceiver. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Mawhinney according to the teachings of Vega to have the second security tag be a radio frequency identification (RFID) tag, said RFID tag further comprising an identification module to provide an identifier for said second security tag and a transmitter to send a signal with said identifier to said transceiver.

Regarding claim 19, Mawhinney discloses all of the claimed limitations except for the claimed security system further comprises a deactivation module to deactivate said first and second security tags. Vega teaches a deactivation system that is in place to deactivate the disposable transponders (both EAS (RF) and RFID) before they are taken through the interrogation zone (col4 46-55). Adding a deactivation system to Mawhinney would allow the users to walk out of the security system with a valid purchase without setting off the alarm and it would cut down on false alarms caused in this manner. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Mawhinney according to the

teachings of Vega to add a deactivation module to deactivate said first and second security tags.

Regarding claim 21, Mawhinney discloses the following claimed subject matters:

The claimed security system wherein one of said security tags is a radio frequency security tag is met by the tag being receptive to RF signals (col1 49-68);

However, Mawhinney does not specifically disclose the claimed security system wherein one of said security tags is a radio frequency identification (RFID) security tag. Vega teaches a combined EAS and RFID tag reader that can detect the presence of both regular EAS (RF) and RFID tags (col4 51-55). The system of Vega interrogates the RFID tag and receives a response signal that contains information that is stored in the RFID tag (col4 51-55) including the tag's identification (col3 42-44). Modifying the system of Mawhinney to be able to detect RFID tags in addition to RF tags would be beneficial because the system would then be able to detect multiple different types of tags. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Mawhinney according to the teachings of Vega to allow the system to detect both RF and RFID tags.

Regarding claim 31, the claim is interpreted and rejected as claim 7 stated above. The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

13. Claims 8, 9, 32 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mawhirran in view of Vega and further in view of Shanahan (US Patent Publication 2004/0148226).

Regarding claim 8, Mawhirran and Vega disclose all of the claimed limitations except for the claimed method wherein said determining comprises decoding said security tag information from said fourth signal, said security tag information comprising an identifier for said second security tag, comparing said identifier to a list of valid identifiers, determining whether said identifier is valid based on said comparison, and sending an alarm signal if said identifier is not valid. Shanahan discloses *Method And Apparatus For Electronic Product Information And Business Transactions* that teaches a security system having an RFID reader that when an RFID tag is detected, the system draws out the RFID tag identifier and compares it to a list of valid items that can pass through the security system and if the identifier does not match then an alarm is sounded (paragraph 51). It would be beneficial to modify the method of Mawhirran and Vega in this manner because it would help to prevent the theft of items along with providing a valuable stock-keeping operation. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Mawhirran and Vega according to the teachings of Shanahan to modify the method wherein said determining comprises decoding said security tag information from said fourth signal, said security tag information comprising an identifier for said second

security tag, comparing said identifier to a list of valid identifiers, determining whether said identifier is valid based on said comparison, and sending an alarm signal if said identifier is not valid.

Regarding claim 9, Mawhirran, Vega and Shanahan disclose all of the claimed limitations. The claimed method comprising receiving said alarm signal and triggering said alarm in response to said alarm signal is met by the alarm being triggered when the identifier is not valid (paragraph 51).

Regarding claim 32, the claim is interpreted and rejected as claim 8 stated above. The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

Regarding claim 33, the claim is interpreted and rejected as claim 9 stated above. The examiner takes official notice that it is well known in the art to use computers and computer related technology (i.e. CPU, memory, etc...) to implement electronic systems.

14. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Mawhirran in view of Vega and further in view of Landt et al. (Landt; US Patent 5,030,807).

Regarding claim 11, Mawhirran and Vega disclose all of the claimed limitations except for the claimed method further comprising receiving a fifth signal in response to said fourth signal, said fifth signal representing said identifier for said second security tag and a second code; storing said second code at said security tag; receiving said second signal at said second security tag; and transmitting a sixth signal from said second security tag in response to said second signal, with said sixth signal representing said identifier for said second security tag and said second code. Landt discloses *System For Reading And Writing Data From And Into Remote Tags* that teaches receiving a signal from a tag including the tag's identifier and recognizing that the tag needs to be written to then sends a signal to the tag to write the new information into the tag (figure 1). It would be obvious that after such a write to the tag, any further interrogation of the tag that would normally receive the first code would now receive the second code as the second code has now been written into the tag, so any interrogation of the tag by the 'second signal' would result in a separate signal response from the tag including the identifier of the tag and the new code stored in the tag. It would be beneficial to modify the device of Mawhirran and Vega to be able to write to the RFID tags in the system in order to modify the contents of the information stored in the tags in order to better serve any number of functions including stock-keeping, price-changing, etc... Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the device disclosed by Mawhirran and Vega according to the teachings of Landt to modify the method to further comprise comprising receiving a fifth

signal in response to said fourth signal, said fifth signal representing said identifier for said second security tag and a second code; storing said second code at said security tag; receiving said second signal at said second security tag; and transmitting a sixth signal from said second security tag in response to said second signal, with said sixth signal representing said identifier for said second security tag and said second code.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Asbrink, USP 4,704,602

Piccoli et al. USPGPUB 2004/0233042

Marsh et al. USP 5,519,381

Purinton et al. USP 4,249,167

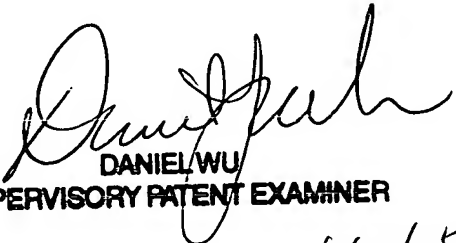
Lauro et al. USP 5,604,485

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Travis R Hunnings whose telephone number is (571) 272-3118. The examiner can normally be reached on 8:00 am - 5:00 pm M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Daniel J Wu can be reached on (571) 272-2964. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TRH


DANIEL WU
SUPERVISORY PATENT EXAMINER
4/04/05